UNITED STATES BANKRUPTCY COURT
EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

In re: Circuit City Stores, Inc., et al., Debtors.	Case No. 08-35653-KRH Chapter 11

CONSUMER PRIVACY OMBUDSMAN

REPORT TO THE COURT

FOR THE SECOND SALE OF CONSUMER DATA

August 26, 2009

Lucy L. Thomson
Consumer Privacy Ombudsman

The Willard; Suite 400
1455 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
(703) 798-1001
lucythomson1@mindspring.com

I. Consumer Privacy Ombudsman Report to the Court

Pursuant to Bankruptcy Code section 332(b), Lucy L. Thomson, the Consumer Privacy Ombudsman ("the CPO") appointed in this case, submits this Report to assist the Court in evaluating and resolving issues related to the protection of the privacy of personally identifiable information (PII) of Circuit City consumers.[1] .

The Bankruptcy Code provides a framework in sections 332 and 363 for evaluating the sale of personally identifiable consumer records in the context of a bankruptcy case. 11 U.S.C. §§ 101 *et. seq*.

Section 363(b) provides:

> 1) The trustee, after notice and a hearing, may use, sell, or lease, other than in the ordinary course of business, property of the estate, except that if the debtor in connection with offering a product or a service discloses to an individual a policy prohibiting the transfer of personally identifiable information about individuals to persons that are not affiliated with the debtor and if such policy is in effect on the date of the commencement of the case, then the trustee may not sell or lease personally identifiable information to any person unless—
>
> (A) such sale or such lease is consistent with such policy; or
>
> (B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease—
>
> (i) giving due consideration to the facts, circumstances, and conditions of such sale or such lease; and
>
> (ii) finding that no showing was made that such sale or such lease would violate applicable non-bankruptcy law.

Section 332(b) provides:

> The consumer privacy ombudsman may appear and be heard at such hearing and shall provide to the court information to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale or lease of personally identifiable information under section 363(b)(1)(B). Such information may include presentation of--
>
> (1) the debtor's privacy policy;
>
> (2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court;

[1] The Court entered an order on April 10, 2009 authorizing the U.S. Trustee to appoint the CPO.

(3) the potential costs or benefits to consumers if such sale or such lease is approved by the court; and

(4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers.

This Report addresses each of the requirements for a bankruptcy sale of personally identifiable Circuit City consumer records. During the past two weeks, the CPO has received input from the Debtors, the Buyers, and a representative of the National Association of Attorneys General (NAAG), and has endeavored to reflect the substance of their views in this Report.

It outlines the considerations that would need to be taken into account by the Court in making this decision. The CPO recommends that the Court approve the sale of the Circuit City customer records to Firemark Investment Ptd Ltd. and to Micro Electronics (a/k/a Micro Center).

Firstmark is a "qualified buyer," and agrees to comply with the Circuit City Privacy Policy, and to provide notice of the sale and an opportunity for consumers to opt out. In accordance with the Privacy Policy, Firstmark has agreed not to sell or lease the consumer data to any third party company for their marketing purposes. Therefore, the Privacy Policy has not been violated, and no non-bankruptcy law has been violated.

Micro Center is a "qualified buyer," who is purchasing the Circuit City Alpine Data, which was collected from consumers in the Circuit City stores. These records are not covered by any privacy policy. Therefore, no Privacy Policy has been violated, nor has any non-bankruptcy law been violated.

The CPO has worked with the two Buyers to develop Privacy Protections for all Circuit City consumers. These will be presented for the Court's consideration at the August 27, 2009 hearing. If approved, they will be made a part of each of the final Sale Orders.

II. Request to Sell Personally Identifiable Consumer Information [2]

Circuit City was a leading retailer of consumer electronics, home office products, entertainment software, and related services. As of August 2008 the company operated 715 stores in 158 U.S. media markets. The company maintained a website at www.circuitcity.com where it sold its merchandise online. Circuit City, through non-debtor affiliates, also sold consumer electronics in 502 company-owned stores and 270 dealer outlets in Canada. The international segment operated a website at www.thesource.ca.

Circuit City customers were able to shop in its stores, on the Web, and by telephone. The major categories of products and services included video, information technology, audio, entertainment, warranty, services (mobile and home theatre installation and product repairs) and third parties for services subscriptions.

On November 10, 2008, Circuit City Stores West Coast, Inc., and Circuit City Stores, Inc. (the "Sellers" and, collectively with the debtors and debtors in possession in the above-captioned jointly administered cases, the "debtors"), filed voluntary petitions for relief under Chapter 11 of Title 11 of the United State Code, 11 U.S.C. §§ 101 *et. seq*. ("the Bankruptcy Code"). On January 16, 2009,

---

[2] Section 101 (41A) of the Bankruptcy Code defines the term "personally identifiable information" to mean--

(A) if provided by an individual to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes--

(i) the first name (or initial) and last name of such individual, whether given at birth or time of adoption, or resulting from a lawful change of name;

(ii) the geographical address of a physical place of residence of such individual;

(iii) an electronic address (including an e-mail address) of such individual;

(iv) a telephone number dedicated to contacting such individual at such physical place of residence;

(v) a social security account number issued to such individual; or

(vi) the account number of a credit card issued to such individual; or

(B) if identified in connection with 1 or more of the items of information specified in subparagraph (A)--

(i) a birth date, the number of a certificate of birth or adoption, or a place of birth; or

(ii) any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically.

Circuit City announced that it was shutting down. Store closing sales were held from January 17, 2009 to March 8, 2009.

A. First Sale of Circuit City Customer Records

On April 5, 2009, the Sellers executed an Asset Purchase Agreement with Systemax Inc. (the "Purchaser" or Buyer"), the "Stalking Horse Bidder." Systemax Inc. (NYSE: SYX), a Fortune 1000 company, is a leading retailer of brand name and private label products, including personal computers, notebook computers, consumer electronics, computer-related accessories, technology supplies and industrial products.

The Court approved the sale of the Intellectual Property and Internet Assets of Circuit City to Systemax. This included records of:

- approximately 14,000,000 Circuit City consumers (i) who transacted purchases on circuitcity.com and (ii) other customers for whom Circuit City has an e-mail address without a web transaction, whether the customer created an account on the website or provided his/her e-mail address at point of sale in a store or phone transaction (the "Circuit City Data"), and
- approximately 33,000,000 Circuit City consumers who made purchases in a retail store or by telephone (the "Alpine Data").

B. Second Sale of Circuit City Customer Records

At a hearing held on July 16, 2009, the Court approved Procedures in connection with the Sales of Miscellaneous IP Property, including the second sale of Circuit City customer records. The Debtors conducted four auctions on August 18 at which they received 13 bids for various IP assets from 12 different bidders.

Records to be Sold -- The Debtors have secured two asset purchase proposals for the sale of Circuit City personally identifiable consumer information.

1) **Firstmark**

Sale of the Firedog and IQ Crew PII -- The PII consists of that portion of the Alpine Data for the approximately two million consumers who made a purchase of Firedog branded goods or services. *Alpine Data* was collected by Circuit City via the Sellers' retail channels other than the circuitcity.com website. FireDog.com delivered electronic and technology technical services for broken home theater, tv, pc or car electronics. They offered a variety of technicians who specialized in electronics and technology products, including pc, protect, repair, improve, home theater services, installation and services, car electronics services, car audio and mp3, GPS navigation, mobile video, satellite radio and others. Customers were encouraged to sign up for updates and news by submitting their e-mail address on the newsletter application box on the website.

2) **Micro Electronics** (a/k/a **Micro Center**)

Sale of the Alpine Data -- Alpine Data consists of records of approximately 33,000,000 Circuit City consumers who made purchases in a retail store or by telephone (the "Alpine Data"). It contains certain PII, including: name and address, telephone number, information about products purchased from the Debtors, and some demographic information. These records are not covered by any privacy policy and were sold to Systemax on a non-exclusive basis. Micro Electronics is purchasing the Alpine Data on an exclusive basis, except for the prior sale to Systemax. Thus, this is the last and final sale of the Alpine Data.

Sale of Trading Circuit IP and the Trading Circuit Data -- As of 2006 or 2007, Trading Circuit operated as a business-to-business network similar to Ebay; however, previously, it also operated as a business-to consumer network. The assets to be sold include (a) information concerning business-to-business transactions and (b) information concerning business-to-consumer transactions. The database includes information concerning 65,000 persons or entities, including

name, address, email and purchase history for these persons/entities.

Records Not Included in the Sale

Customer Financial Information and Credit Card Numbers -- Representatives of Circuit City have confirmed that these data do not include consumer financial information, payment account numbers, or personal identification numbers of individuals.

III. Circuit City Privacy Policy

Circuit City published a Privacy Policy on its website at www.circuitcity.com. The Privacy Policy only pertains to information collected online. It does not apply to information collected from customers in the Circuit City retail stores. Thus, the Alpine Data is not subject to the Privacy Policy.

The Firedog data is covered by the Circuit City Privacy Policy.

Information Shared with Third Parties -- The Circuit City Privacy Policy contains the following statement about sharing of consumer information with third parties for their marketing purposes:

> "We do not rent, sell or exchange your information or other personally-identifiable information to third-party companies for their marketing purposes."

IV. CPO Process and Applicable Non-Bankruptcy Laws

Section 332 of the Bankruptcy Code makes the protection of consumer privacy an important focus of all bankruptcy proceedings in which personally identifiable consumer records are to be sold. The statute provides a broad mandate for the Consumer Privacy Ombudsman – to investigate and provide the Court with information relating to:

- The Debtor's Privacy Policy,
- Potential losses or gains of privacy to consumers if the sale is approved,
- Potential costs or benefits to consumers if the sale is approved, and

- Possible alternatives that would mitigate potential privacy losses or costs to consumers.

11 U.S.C. § 332 (2007).

A. Analytical Framework

Section 363(b)(1) of the Bankruptcy Code provides that the Court must make a number of determinations before the Trustee is authorized to sell the personally identifiable Circuit City consumer records. More specifically:

- If the debtor's Privacy Policy prohibits the transfer of personally identifiable information about individuals to persons that are not affiliated with the debtor; and
- If the policy is in effect on the date of the commencement of the case,
- Then the Trustee may not sell personally identifiable information to any person unless--

  (A) such sale is consistent with such policy; or

  (B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease --

    (i) giving due consideration to the facts, circumstances, and conditions of such sale; and

    (ii) finding that no showing was made that such sale would violate applicable non bankruptcy law.

B. Core Issues

Initially the analysis should focus on the Circuit City Privacy Policy and its legal ramifications. The Court must determine if the Privacy Policy has been violated. If the Privacy Policy has not been violated, the sale may simply proceed. If the Privacy Policy has been violated, the sale may proceed only if no applicable non-bankruptcy law has been violated.

Even if the Privacy Policy is violated, the Court can approve this sale of the personally

identifiable consumer records if:

- Consent is obtained from each customer, or
- The CPO process is followed, and
- The Court finds that no applicable non-bankruptcy law has been violated.

In this case, the legal analysis is different for the two Buyers.

Firstmark has agreed to comply with the Circuit City Privacy Policy, and to provide notice of the sale and an opportunity for consumers to opt out. Firstmark agreed not to sell or lease the consumer data to any third party company for their marketing purposes. Therefore, the Privacy Policy has not been violated, and no non-bankruptcy law has been violated.

Micro Center is purchasing the Circuit City Alpine Data, which was collected from consumers in the Circuit City stores. These records are not covered by any privacy policy. Therefore, no Privacy Policy has been violated, nor has any non-bankruptcy law been violated.

Consideration of whether the Privacy Policy has been violated should be evaluated in light of the Fair Information Practice Principles, widely-accepted principles established by the Federal Trade Commission (FTC) that govern the collection, use, and transfer of personally identifiable information. They explain many important privacy concepts that govern the analysis.

C. Fair Information Practice Principles

The FTC has studied the manner in which entities collect and use personal information -- their "information practices" -- and the safeguards required to assure those practices are fair and provide adequate privacy protection. The FTC has identified widely-accepted principles concerning fair information practices. [3] Common to these are five core principles of privacy protection. These core principles provide a useful framework for analyzing the privacy issues presented in this case. This section of the CPO Report identifies each of the FTC principles and discusses the practical

[3] FTC, Fair Information Practice Principles, *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm

considerations applicable to the facts of the Circuit City case. The FTC principles and their explanatory material are set forth in italics.

(1) ***Notice/Awareness***

> *The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below -- choice/consent, access/participation, and enforcement/redress -- are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.*

Circuit City: When it launched its e-commerce website in 1999, Circuit City published a Privacy Policy on its website at www.circuitcity.com. The CPO has been informed that other than updating factual information such as the names of its business partners, the Privacy Policy has not been changed in any material respect since that time. This Privacy Policy only pertains to information collected online and not to information collected in the Circuit City stores.

Adherence to the Privacy Policy: Once consumers are notified of their rights through the Privacy Policy, these rights must be honored. There are differing views about whether the sale of the personally identifiable Circuit City consumer records violates the Circuit City Privacy Policy. The operative language at issue is the following:

> "We do not rent, sell or exchange your information or other personally-identifiable information to third-party companies for their marketing purposes."

Even if that section of the Privacy Policy is violated, the Court can approve this sale of the personally identifiable consumer records if:

- Consent is obtained from each customer, or
- The CPO process is followed, and
- The Court finds that no applicable non-bankruptcy law has been violated.

Consistent with the Privacy Policy, consumers must be provided notice that their data is being

sold in the Circuit City bankruptcy case. The CPO recommends that this be accomplished in three ways: Notice to consumers on the website, by postal mail, and by e-mail: Notice should be provided to all consumers with a clear and conspicuous notice on the Micro Center websites of the change of corporate ownership and of their right to Opt Out of the transfer of their personally identifiable information and/or of receiving future e-mail communications.

Substitute Notice to Consumers: Although Circuit City has postal addresses for most of the individuals in its database, it does not have e-mail addresses for all of the consumers in the "Alpine Data." Notice by postal mail would be prohibitively expensive. [4] The CPO recommends that the consumers in the "Alpine Data" receive what is known as "substitute notice." This concept is a central part of the state data breach notification statutes; it may be accomplished by a clear and conspicuous posting of a notice on the home page of the Micro Center website, or publication in or broadcast through media. It is justified if the cost of providing written notice is substantial, or the affected class to be notified is a large number of people (exceeds 500,000 people), or the organization does not have sufficient contact information to provide notice.

(2) ***Choice/Consent***

> *At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Choice relates to secondary uses of information* -- i.e., *uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.*
>
> *Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out.*
>
> ***Opt-in*** *regimes require affirmative steps by the consumer to allow the collection and/or use of information*

[4] It appears that notification by postal mail would not financially feasible -- bulk mail at $.50 per piece x 33,000,000 would cost $16,500,000 or at $.25 (postcard) would be $8,240,000.

Opt-out *regimes require affirmative steps to prevent the collection and/or use of such information.*

In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

On what basis should the decision be made about whether an Opt In or an Opt Out process should be selected?

While Opt In provides the strictest protection for consumers, it would likely result in a huge and unwieldy undertaking in the context of this bankruptcy sale that might be cost-prohibitive and could result in a significant delay of the sale.

Data Sensitivity: An Opt In approach is usually reserved for the sale or transfer of the most sensitive types of consumer data. The State Attorneys General in the *Toysmart* case made the point in opposing the sale of data about children and of credit card records that "Because the information collected about consumers on Toysmart's Web site likely includes information collected from children, the information should be considered sensitive… For this reason, the higher, opt in standard should apply." [5] In this Circuit City sale, the personal records are less sensitive – they include name, address, telephone number, e-mail addresses of some consumers, and purchasing history. Some of this information is available from public sources, including public telephone books. For example, at www.whitepages.com, a user can enter a name and city and the website will provide the individual's address and telephone number. The reverse can also done – entering a street address will produce the name and telephone number.

The State data breach notification laws are instructive in providing a definition of sensitive data that, if compromised, could expose consumers to potential identity theft and fraud and therefore must

[5] In re Toysmart.com LLC, No. 00-13995-CJK (U.S. Bankruptcy Court, D. Mass.), Objection of the Commonwealth of Massachusetts and 46 States to the Debtor's Motion to Approve Settlement with Federal Trade Commission and for Authority to Enter in Consent Agreement, page 8.

be well protected. This personal data includes (i) a person's first name or initial and last name, plus (ii) one of the following data elements: social security number, driver's license number, or financial account or credit or debit card number. Using the States' definitions of sensitive data, the personal Circuit City Data to be sold does not rise to the level of requiring an Opt In notification to consumers. The CPO recommends Opt Out Notice to consumers as appropriate and practical in this case.

(3) Access/Participation

> *This refers to an individual's ability both to access data about him or herself* -- i.e.*, to view the data in an entity's files -- and to contest that data's accuracy and completeness.*

Circuit City: Under its Privacy Policy, Circuit City provides an opportunity for consumers to create an Account on the website and to make changes to it.

(4) *Integrity/Security*

> *To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.*
>
> *Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.*

Circuit City: The CPO has focused on information security as critical to protect the personally identifiable consumer records and recommends that the Buyer agree to employ appropriate information security controls (technical, operational and managerial) to protect the personally identifiable customer information, including strong encryption**.**

(5*) Enforcement/Redress*

> *The core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.*

Circuit City: Since the Court would be supervising the transaction, it has all the powers available to the federal bankruptcy court to enforce it orders, and specifically over whatever provisions are included in the Sale Order. The recommendations in this CPO Report are designed to enforce the

core privacy principles.

D. Non-Bankruptcy Laws

1. Unfair or Deceptive Practices

Section 5 of the Federal Trade Commission (FTC) Act, which prohibits "unfair or deceptive practices in or affecting commerce [.]", the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley (GLB) Act, provide privacy protections for the PII of consumers in the United States. Cases brought by the FTC define the approach to privacy that is analogous to the issues in this case.[6] In this sale, the question may be posed as to whether the transfer of the records to the Buyer constitutes an unfair or deceptive business practice.

Section 5 of the FTC Act (FTCA) prohibits "unfair or deceptive practices in or affecting commerce [.]" 15 U.S.C. § 45(a). "Unfair" practices are defined by the FTC as those that "cause[] or [are] likely to cause *substantial injury* to consumers which *is not reasonably avoidable* by consumers themselves and *not outweighed by countervailing benefits* to consumers or to competition" (15 U.S.C. Sec. 45(n)). [7]

There is no single definition for the phrase "unfair business practices." It is an evolving concept reflecting the ingenuity of unscrupulous business persons in concocting new schemes to gain advantage at someone else's expense. The existence of an unfair business practice is a question of fact determined in light of all the circumstances surrounding a case.

In an attempt to set some standards, the FTC identified several factors to be considered in

---

[6] *See generally* Federal Trade Commission, Privacy Initiatives, *available at* http://www.ftc.gov/privacy/index.html (last viewed November 26, 2008). An analogous case to this one is *In re Toysmart.com*, in which the FTC and the Debtor filed a Stipulation and Order Establishing Conditions on the Sale of Customer Information with the United States Bankruptcy Court for the District of Massachusetts. *In re Toysmart.com, available at* http://www.ftc.gov/os/2000/07/toysmarttbankruptcy.1.htm. The State Attorneys General objected, arguing that because sensitve records about children and credit card numbers were being sold, consumers should be permitted to consent to the sale through an Opt In procedure. Because the records were not sold within a specified period of time, they were destroyed.

[7] *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority, Enforcement Authority*, Consumer Protection, *available at* http://www.ftc.gov/ogc/brfovrvw.shtm.

determining whether a practice is unfair: (1) whether the practice offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers. These criteria have been accepted by states that have adopted their own counterparts to the FTCA. *See, e.g., People v. Casa Blanca Convalescent Homes, Inc.*, 159 Cal. App. 3d 509, 530; 206 Cal. Rptr. 164 (1984); *Brown Daltas & Assocs. V. General Accident Ins. Co.*, 844 F. Supp. 58 (D. Mass. 1994), *rev'd. on other grounds*, 48 F.3d 30 (1st Cir. 1995), *cert. den*., 516 U.S. (1995); *Harris v. NCNB Nat'l. Bank*, 85 N.C. App. 669, 355 S.E.2d 838 (1987).

As specifically set forth in federal statute, *i.e*., 15 U.S.C. § 45 (n) granting the FTC its authority, an act or practice is unfair [8] if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." See, *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1363-66 (11th Cir. 1988); *also see, FTC v. J.K. Publications, Inc.*, 99 F. Supp. 2d 1176, 1201 (C. D. Ca. 2000). [9] Thus, to find unfairness, there must first be an identifiable injury. If so, the injury must satisfy three tests: (1) it must be substantial; (2) it must not be outweighed by countervailing benefits to consumers or competition; and (3) it must be one that consumers themselves could not reasonably have avoided. [10] *Orkin* at 1364 (citing FTC's 1980 Policy Statement). As such, the FTC is without authority to address unfair or deceptive business practices that do not meet these standards defining "injury." In sum, the injury must be substantial, outweigh any countervailing benefit to the consumer, and be one

[8] Many cases use the terms "deceptive" and "unfair" synonymously -- without significant distinction.
[9] This definition is derived from a letter which the FTC wrote to Senators Danforth and Ford when Congress was considering an amendment to section 5 which would have defined unfair acts and practices. *See* A.F.S., 767 F.2d at 970 (D.C. Cir. 1995). Commonly referred to as the FTC's "Policy Statement" on the meaning of unfair acts and practices, the text of this letter is reprinted in H.R.Rep. No. 156, Pt. 1, 98th Cong., 1st Sess. 33-40 (1983), and Trade Reg.Rep. (CCH) ¶ 50,421 at 55,947-51.
[10] 15 U.S.C. 57(a)(1)(B) authorizes the FTC to promulgate "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce." The FTC has done so in many subject areas. *See, e.g.*, 16 CFR 18.3 (nursery industry).

the consumer cannot reasonably avoid.

In this sale, it is unclear if there is any injury at all. No credit card numbers are involved; no social security numbers – only name, address, and in some cases e-mail address. The majority of the addresses in the Alpine data are postal addresses. Thus, the worst that can happen to consumers whose data is sold to Micro Center is that they will receive some unwanted mail, which they are free to place in the trash. Consumers may easily discard any mailings or "opt out" of any e-mails they may receive as a result of yet further opt out provisions. As such any "violation" of the privacy policy statement is "minimal" or "technical" in nature – and cannot be viewed as "substantial," as required by the FTC.

The second prong of the test focuses on countervailing benefits to the consumer or competition. Micro Center represents that it will offer discounts and other benefits to consumers purchasing its electronic products. Such advertising may also serve to foster competition by encouraging other electronic businesses to offer yet further benefits and price reductions.

Consumers may avoid contact with Micro Center by initially or later opting out of any contact with the company. " 'Consumers may act to avoid injury before it occurs if they have reason to anticipate the impending harm and the means to avoid it, or they may seek to mitigate the damage afterward if they are aware of potential avenues toward that end.' " *Orkin* at 1365 (quoting *FTC v. Orkin Exterminating Co.*, 108 F.T.C. 341, 366 (1986)). Here, all consumers have the power to avoid contact with the Buyer and any of its advertising.

2. Financial Information and Credit Card Numbers

Federal law protects financial information, including credit card numbers, and provides certain requirements for providing notice of an organization's privacy policy and an opportunity for consumers to opt-out of changes to that policy.

Title V, subtitle A, of the Gramm-Leach-Bliley Act requires the FTC, along with several other

agencies, to issue regulations (see 16 CFR Part 313) ensuring that financial institutions protect the privacy of consumers' personal financial information. Such institutions must develop and give notice of their privacy policies to their own customers at least annually and before disclosing any consumer's personal financial information to an unaffiliated third party, must give notice and an opportunity for that consumer to Opt Out from such disclosure. The subtitle also requires the FTC and other agencies to issue regulations (*see* 16 CFR Part 314) for the safeguarding of personal financial information. The Act also limits the sharing of account number information for marketing purposes. Subtitle B of Title V prohibits obtaining customer information of a financial institution by false pretenses. [11]

In this case, the data do not include consumer financial information, payment account numbers, or personal identification numbers of individuals. Circuit City does not retain any such information and is not subject to GLB. As such, the sale of credit card or other financial information is not an issue here.

3. Children's Online Privacy Protection Act (COPPA)

COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, or disclosure of PII from or about children under age 13 obtained on the Internet. Circuit City explicitly states on its website that it does not collect information from children.

> "Circuit City is committed to preserving online privacy for all its website visitors, including children. Circuitcity.com is a general audience site, and we do not knowingly collect information about children or sell products to children. Consistent with the Children's Online Privacy Protection Act, we will not knowingly collect any information from or sell product to children under the age of 13. If you are under the age of 13, you much ask your parent or guardian to assist you in using circuitcity.com."

There is no evidence that the Circuit City sale is not in compliance with the requirements of COPPA.

[11] The Securities and Exchange Commission has proposed amendments to Gramm-Leach-Bliley and the Fair Credit Reporting Act entitled Privacy of Consumer Financial Information and Safeguarding Personal Information, Proposed Rule -- Part 248-Regulation S-P: RIN 3235-AK08, *available at* http://www.sec.gov/rules/proposed/2008/34-57427.pdf (last viewed November 26, 2008).

4. State Laws

Nearly all states that have enacted "Little FTC" statutes appear to predicate standing to maintain a private action on actual injury resulting from the alleged offending business practice. Because some of these statutes provide for the recovery of compensatory or punitive damages, a party's ability to bring an action depends on showing an injury proximately caused by the defendant's conduct, as in any other tort action. Typical of such statutes is Louisiana's, which confers a right of action on both a consumer and a business competitor "who suffers any ascertainable loss of money or movable property, corporeal or incorporeal" from unlawful business practices. LSA-RS § 51:1409; *see also*, *Monroe Medical Clinic, Inc. v Hospital Corp. of America*, 522 So. 2d 1362 (1988).

In general, harm is a core requirement of these statutes. Since the sale of the information documents here result in little or no harm to consumers, these laws cannot act as a bar to this sale.

5. Data Breach Notification Laws

Forty five (45) states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws that require any business in possession of certain sensitive personal information about a covered individual to disclose any breach of that information to the person affected. [12] The laws are similar in structure, approach, content and terminology. By requiring notice to persons who may be adversely affected by a security breach (e.g., persons whose compromised personal information may be used to facilitate identity theft), these laws seek to provide such persons an opportunity to take steps to protect themselves against the consequences of identity theft. There are several reasons why the state data breach notification laws do not apply in this case. [13]

---

[12] National Conference of State Legislatures, *State Security Breach Notification Laws* (as of December 16, 2008), *available at* http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

[13] The FTC has recently brought lawsuits in a number of cases involving data breaches that posed serious risks to consumers. DSW Inc. Settles FTC Charges, *available at* http://www.ftc.gov/opa/2005/12/dsw.shtm; CardSystems Solutions Settles FTC Charges, *available at* http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm; Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for

In this case, information being sold by Circuit City is not within the definition of covered personal information. The sale of the Circuit City consumer information is not a "Breach" as defined in the statutes. There is no basis to argue that the sale of the relevant information here constitutes a "data breach."

6. Do-Not-Call Registry Act of 2003, 15 U.S.C. § 6102

The "Do-Not-Call" Act authorizes the FTC under section 3(a)(3)(A) of the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6102(a)(3)(A), to implement and enforce a do-not-call registry. The Act also ratified the do-not-call registry provision of the FTC's Telemarketing Sales Rule, 16 C.F.R. 310.4(b)(1)(iii), which became effective on March 31, 2003. [14]

The States have similar Do-Not-Call and "no spam" (unsolicited commercial or bulk e-mail) statutes.[15] In this case, the Buyers have agreed to comply with the "do-not-call" and "no spam" laws by ensuring that they do not call any telephone numbers on the "do-not-call" and "no spam" lists for marketing.

These laws do not prohibit ownership of numbers on the do-not-call list. It is the responsibility of the Buyers to use the numbers for a lawful purpose and in compliance with federal and state laws. Any Buyer will be under an obligation to comply with these laws – not merely with the purchased records but with any other records it may have or obtain containing any PII.

In my view, there is no legal impediment to the sale of telephone numbers of Circuit City consumers.

Failing to Provide Adequate Security for Consumers' Data, *available at* http://www.ftc.gov/opa/2008/03/datasec.shtm; Proposed settlement involving The TJX Companies, Inc. and Fifth Third Bancorp ("Defendants"), U.S. District Court for the District of Massachusetts, *available at* www.TJXsettlement.com.

[14] Federal Communications Commission, National Do-Not-Call Registry, *available at* http://www.fcc.gov/cgb/donotcall/.

[15] National Conference of State Legislatures, State Do-Not-Call Statutes, *available at* http://www.ncsl.org/programs/lis/CIP/donotcall.htm; State Laws Relating to Unsolicited Commercial or Bulk E-mail (SPAM), *available at* http://www.ncsl.org/programs/lis/legislation/spamlaws02.htm

VII. Recommendations

A. Firstmark is a "Qualified Buyer"

The CPO believes that Firstmark should be found to be a "qualified buyer" because it meets the following criteria:

- A Buyer in materially the same line of business as Circuit City (*i.e.*, who concentrates its business in the sale of personal computers, computer supplies, and consumer electronics).
- Firstmark agrees to use the personally identifiable consumer records for the same purpose(s) as are specified in the Circuit City Privacy Policy.
- Firstmark agrees to comply with the Circuit City Privacy Policy and its specified policies and practices.
- Firstmark agrees that prior to making any "material change" to the Privacy Policy, or the use or disclosure of personal information different from that specified in the Privacy Policy, it will notify consumers by e-mail (if available) and a notice on the website, and afford them an opportunity to Opt Out of the changes to those policies or the new uses of their personal information.
- Firstmark agrees to notify Circuit City customers of the change in corporate ownership by placing a clear and conspicuous notice on the home page of the website. This notice will be maintained for one year from the date of the closing.
- Firstmark agrees to continue the Circuit City practice of providing consumers with opportunities to Opt Out of receiving e-mail and postal mailings of advertisements and notices of promotions and special product offerings.

- Firstmark agrees to employ appropriate information security controls (technical, operational and managerial) to protect the personally identifiable customer information, including strong encryption**.**
- Firstmark agrees to abide by any applicable federal, state or international laws, including laws prohibiting unfair or deceptive practices "UDAP," data breach, privacy, "do-not-call," and "no spam" laws.

B. Micro Center is a "Qualified Buyer"

The CPO believes that Micro Center should be found to be a "qualified buyer" because it meets the following criteria:

- A Buyer in materially the same line of business as Circuit City. Micro Center is a nationwide retailer and website of 30,000 technology-related items and exciting product offers.
- Micro Center agrees to use the personally identifiable consumer records for the same purpose(s) as are specified in the Circuit City Privacy Policy.
- Micro Center agrees to voluntarily extend privacy protections to the former customers of Circuit City by covering them under the Micro Center Privacy Policy.
- Micro Center agrees to notify consumers by postal mail, e-mail (if available) and a notice on the website of the change of corporate ownership and of the customers' right to opt-out of the transfer of their personally identifiable information to Micro Center and/or to receive future postal mail or e-mail communications from Micro Center or its partners.
- Micro Center agrees to continue the Circuit City practice of providing consumers with opportunities to Opt Out of receiving e-mail and postal mailings of advertisements and notices of promotions and special product offerings.

- Micro Center agrees to employ appropriate information security controls (technical, operational and managerial) to protect the personally identifiable customer information, including strong encryption**.**
- Micro Center agrees to abide by any applicable federal, state or international laws, including laws prohibiting unfair or deceptive practices "UDAP," data breach, privacy, "do-not-call," and "no spam" laws.

The sale of personally identifiable consumer data to Micro Center presents some practical issues that should be considered. First, the consumer data in the Alpine database was collected in the stores and is not covered by the Circuit City Privacy Policy. However, Micro Center has voluntarily agreed to extend privacy protections to all 33,000,000 consumers. The details of these protections are contained in the final Sale Order (and will be filed as an Exhibit to this CPO Report). Ideally, to provide a high level of maximum privacy protections, consumers should be notified of the sale and the change of corporate ownership and given an opportunity to opt-out of the transfer of their personally identifiable information to Micro Center and/or to receive future postal mail or e-mail communications from Micro Center or its partners. Such an opt-out process by mail would be prohibitively expensive because most of the contact information consists of postal addresses rather than e-mail addresses.

Micro Center has agreed to notify consumers through the promotional mailings they plan to send to about one third of the individuals in the Alpine database. That means about 22,000,000 consumers will not receive direct notice of the sale. They will receive "substitute notice" if they happen to see it the notice of the sale on the Micro Center website. In light of the fact that they are not covered by the Circuit City Privacy Policy, however, this would be reasonable under the circumstances.

Micro Center plans to lease sections of the consumer data to a "very limited number of reputable marketing partners who provide special services or products" that may be of interest and value. Consumers will be notified in these mailings of their right to opt out of future mailings, but not of their right to opt out of having their information ever shared with third parties. However, the extent of the harm is minimal because they can readily dispose of whatever mail they receive if they are not interested in receiving it. On the other hand, having shopped at Circuit City and given their likely interest in electronics, Micro Center may provide them with valuable information, discounts and benefits that may be of benefit to them.

With no legal requirement or Privacy Policy to enforce, on balance, the voluntary actions of Micro Center to extend privacy protections to these consumers is welcome and should be commended.

VIII. Conclusions

The issues related to the proposed sale of the personally identifiable Circuit City consumer records required under sections 332 and 363 of the Bankruptcy Code have been addressed and presented in this CPO Report for the consideration of the Court. A CPO has been appointed, a hearing is scheduled to be held on August 27, 2009, the Court has been advised of the issues regarding compliance with the Circuit City Privacy Policy, and an analysis has been provided of the losses or gains, and costs or benefits to consumers if the sale is approved, and the application of the non-bankruptcy laws.

With respect to the section 332(b) provision that requires assessment of "possible alternatives that would mitigate potential privacy losses or costs to consumers" from the sale, the CPO believes that on balance and in the context of this bankruptcy sale, the recommendations proposed in this Report would protect the privacy rights of Circuit City consumers to the extent possible.

In addition, if the recommendations proposed in this Report are adopted, privacy protections

would be expanded to the consumers in the Circuit City Alpine Data who were not covered previously by the Circuit City Privacy Policy.

Further, the CPO process has ensured that strict limitations are imposed on data to be sold by eliminating all records that could expose consumers to identity theft and fraud, including financial records, and credit card and personal identification numbers.

In summary, the CPO believes that the Recommendations in this Report strike an appropriate balance between the privacy rights of consumers and practical considerations associated with this bankruptcy sale.

The CPO will stands ready to provide whatever further analysis or recommendations the Court deems appropriate.

Respectfully submitted,

/s/ Lucy L. Thomson

Lucy L. Thomson
Consumer Privacy Ombudsman